accordance with MPEP § 608.02(v), and accompanied by a separate letter to the Official Draftsperson pursuant to MPEP § 608.02(r). The Examiner's comment in the pending Office action to the effect that "[n]umbers do not count as labels" strongly suggests that the Examiner has not reviewed Applicant's proposed drawing corrections. Accordingly, such action is respectfully requested. A copy of the proposed drawing corrections is attached hereto as Exhibit A for the Examiner's convenience. Formal drawings incorporating the proposed corrections will be filed after a Notice of Allowance is received.

Claim 54, 55 and 51 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg (U.S. 6,240,091) in view of Schneier. Claims 56-74 and 82-102 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg in view of Schneier as applied to claims 54, 55 and 81, and further in view of Walker (U.S. 6,263,438). Claims 75-80 and 103-116 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg in view of Schneier and Walker as applied to claim 54, and further in view of Thompson (U.S. 6,282,552). With respect to claims 54-80, canceled by way of amendment on May 27, 2003, these rejections are moot. With respect to claims 81-116, Applicant respectfully traverses these rejections.

(1) In examiner's Office action dated 9/29/2003, Page 2, response to arguments, item #2, the examiner stated that "Applicant's main argument is that the cited prior art does not show one of the entities in the transaction uniquely generating the session key. The Woo-Lam protocol does indeed show one of the parties to the transaction receiving the session key from a third party. However, there is no explicit teaching of why external generation of the session key is beneficial to the system."

Applicant's response:

(A) Applicant's main argument is actually that Chen's system involves only two parties whereas Woo-Lam's system involves three. They use different steps and different trust relationships to complete their respective transactions. They are both secure but very incompatible and entirely different.

(B) It is not clear what the term "external generation of the session key" is referring to. In Woo-Lam's system, all three parties are needed to complete their transaction. Trent is not "external" to the system but rather a pivotal part of the system.

to enable the participants to securely exchange keys and other information in order to complete their unspecified intended purpose, such as on-line purchase. This "intended purpose" – very unfortunately also termed a "transaction" in the literature, can be anything and is not important to the discussion here. Excluding Trent from Woo-Lam's system would not make it a two-party system similar to Chen's system, but would rather render the entire Woo-Lam system inoperable.

(2) On page 3, item #5, the examiner stated that: "In lines 51-67 of column 7, Ginzboorg et al. present a smart card that includes, among other pieces of data, the public key of a second party." "Schneier shows, in step 3, Alice initiating communications with Bob by encrypting a message with Bob's public key and sending it to him. He then encrypts Trent's signature with Alice's public key....."

Applicant's response:

(A) When evaluating a system, we have to look at the system as a whole, not just individual steps. Once again, it is clearly indicated in these statements that Woo-Lam is a three-party system and it would not have worked without Trent. First of all, step 3 would not have been possible without step 1 and 2. And without Trent's signature, the rest of Woo-Lam's (step 4-8) system would not have worked as clearly indicated by the examiner's own statement above. This three-party system is quite different from Chen's two party system.

(B) In lines 51-67 of column 7, Ginzborg et al. indeed suggested the use of a smart card that included the public key of a second party by stating that " it is possible to store the smart card, for example, the key of the charging server so that it can be ensure that the message actually come from the charging server." It is clear form this statement that the storage of the second party public key is for verifying the message signature. The use of this idea over Woo-Lam's system would probably result in the use of a smart card by Alice or Bob to store Trent's public key. But, it would not have reduced Woo-Lam's system into a two-party system or changed its feature in any way. Chen's system puts the second party public key to a much wider and sophisticated use. The system resulting from Woo-Lam in view of Ginzboorg et al. in this case would not have anticipate Chen's system in any way.

(3) On page 3, item #5, the examiner suggested two vulnerabilities in Woo-Lam's system and discussed the possibility of having Bob generating the session key.

Applicant's response:

(A) Woo-Lam's vulnerabilities make Chen's system superior.

(B) Again, Trent is not external to the system but rather part of the system. His role is not limited to session key generation but rather "the center" of the system. In step 1, Alice has to register the intended transaction with Trent by giving Trent both hers and Bob's identity. Both Alice and Bob get each other's public key form Trent. Within the context of the Woo-Lam system, Trent's trustworthiness is not theoretical but rather a requirement for the system to work. The protection of the session key and exchange public key/session key information to Alice and Bob is the main purpose of the system, not a coincidental one. The interactions of the three parties in Woo-Lam system make the exchange of Alice and Bob's public keys and session key secure and possible. Chen's system does not use three parties.

(C) As suggested by the examiner, the party in a system that is given the task of generating a session key sometimes is a trade-off between risks. However, this party is always an integral part of the algorithm. In Chen's system, the session key generation is part of its algorithm, not an arbitrary decision. It is dictated by the algorithm, not influenced by any prior art.

(D) Giving Bob the task of session key generation would require that Alice, Bob and Trent complete the public key exchange first – since without each other's public key Alice and Bob can not communicate with each other securely. Then through another similar process to exchange the session key between Alice and Bob. This would render the Woo-Lam system inefficient but still not make it a two-party system like Chen's.

(4) On page 4, the last paragraph, the examiner stated that "Ginzboorg and Schneier teach a smart card that contains second entity's public key. The smart card and the second entity authenticate themselves to one another and agree on a symmetric key."

Applicant's response:

(A) It is clear from all the discussions, these statements do not reflect the true nature of Ginzboorg and Schneier 's teaching. The smart card and the second party would not have known how to communicate with one another without the help and supervision

of Trent. Their teaching is actually: "The smart card and second entity, through the help of third party (Trent), authenticated themselves to one another and agree on a symmetric key." This third party is unknown and unused by Chen's system. This makes this system quite different from Chen's two-party system.

(5) One page 4-5, the examiner stated that "Walker et al, teach including digital certificates with messages to provide greater assurance. Therefore it would have been obvious.....to send a certificate with Alice's first message, as taught by Walker et al to provide greater assurance."

Applicant's response:

(A) A digital certificate is issued by a central authority. It contains the public key of the certificate bearer, frequently in clear form, signed by this central authority. It requires a certain trust relationship among different parties and it usually has an expiration date. A public key by itself and a certificate for it usually entail different meaning to the system that employs them. Chen's system uses only the public, not a certificate, and therefore not relying on the trust relationship that comes with a certificate.

(B) It is not clear what "Alice first message" is referring to here – first message to Bob or first message to Trent. However, Trent already has Alice's public key and Bob obtains Alice's public key from Trent. They do not need Alice to send her public key to them and will not accept it even if she does. Neither will they accept the certificate from Alice and it adds no greater assurance since the certificate cannot be verified unless the central certificate authority is made part of the system.

(C) In summary so far: with Walker's teaching added to "Schenier in view of Ginzboorg", there is still a three party system using a smart card and optionally sending a certificate form Alice to Bob or Trent. It is still not a two-party system as suggested by Chen and still quite different from Chen's system. Also, in Chen's system, the sending of the cardholder's public key to the second entity is dictated by the system, not arbitrary. Nor is it inspired by any prior art based on the concept of certificate.

(6) On page 6, the examiner stated that "Thompson et al. show a method by which changes to a document are recorded. This method entails signing all changes."